Кібербезпека систем IP-відеоспостереження:

безпека та захист відеоданих від стороннього впливу

Про те, як захистити систему відеоспостереження від хакерських атак, розповідає Віктор АЛІПОВ, керівник відділу продажів по роботі з телеком-операторами ТОВ «СІТОН ГРУП».

Захист інформації (відеоданих), отриманих з камер IP-відеоспостереження, наразі є ключовим питанням у наших реаліях. Роки війни з країною-агресором показали слабкі місця деяких виробників камер та гостру необхідність забезпечення додаткового захисту систем безпеки. Дуже часто ворог за допомогою кібератак на системи IP-відеоспостереження мав можливість відстежувати результати ракетних обстрілів та пересування нашої військової техніки в окремих містах.

То як все ж таки захистити вашу систему відеоспостереження від майбутніх кіберзагроз? В цій статті я спробую розповісти про найпростіші кроки, які необхідно виконати для захисту вашої домашньої або приватної (корпоративної) системи IP-відеоспостереження.

Атака і протидія

IP-відеокамери можна віднести до пристроїв «Інтернету речей» і тому справедливо слід вважати дуже вразливими до кіберзагроз. Сьогодні в наших реаліях захист відеоданих є одним з пріоритетних завдань. У виробників IP-камер відеоспостереження та програмного забезпечення, які присутні на ринку України, є власні розробки та засоби боротьби з кіберзагрозами, про які мова піде далі у нашій статті.

Компанія ТОВ «СІТОН ГРУП» має сертифікованих фахівців напрямку системи IP-відеоспостереження та кібербезпеки, в портфелі компанії присутні рішення таких відомих світових виробників ПЗ та IP-відеокамер, як AXIS та Milestone Systems, і рішень Cybersecurity Splunk, Cisco, Palo Alto, RSA, CiberArk, FUDO Security.

Захист від кіберзагроз у системах IP-відеоспостереження має бути комплексним рішенням, що поєднує у собі як продукти від провідних світових виробників обладнання та програмного забезпечення IP-відеоспостереження, так і рішень Cybersecurity від лідерів напрямку, а також фахівців служби експлуатації даних систем у замовника (**рис. 1**).

Основні кроки, що їх необхідно зробити для упередження кіберзагроз та хакерських атак насамперед на стороні замовника, мають бути здійснені фахівцями, які займаються безпосередньою експлуатацією системи IP-відеоспостереження. Ці кроки засновані на рекомендаціях провідних світових виробників обладнання та програмного забезпечення.

1. На першому етапі зловмисник (хакер) проводить збір інформації (розвідку) стосовно системи IP-відеоспостереження, веде пошук слабких та вразливих місць. Які контрзаходи можливо застосувати на цьому етапі, щоб протидіяти зловмиснику?

Спробую не вдаватись у глибокі технічні подробиці та максимально просто надати відповідь на це питання, а саме: першим чином замовнику необхідно переконатись у тому, що його система відеоспостереження надійно захищена та невидима для сканування портів. Цього можна досягти за допомогою брандмауерів та систем виявлення вторгнень від лідерів напрямку: Splunk, Cisco, Palo Alto, RSA, CiberArk, FUDO Security (**рис. 2**). Для більш детальної консультації можна звернутись до фахівців ТОВ «СІТОН ГРУП».

2. Наступний за логікою крок – це створення зловмисником шкідливого корисного навантаження (payload) на IT-систему замовника та звичайних користувачів. Тут під атакою будуть в першу чергу поштові сервери, активне мережеве обладнання, а можливо, і USB-входи будь-яких пристроїв замовника.

Протидія – це надійний захист електронної пошти для запобігання фішинговим атакам, часте оновлення та виправлення систем для усунення відомих вразливостей і впровадження надійного контролю над USB-портами та іншими фізичними інтерфейсами.

3. Третя стадія – коли зловмисник порушує захист існуючої системи безпеки замовника. Замовник може захиститися від цих дій, встановивши вдосконалені рішення для захисту кінцевих

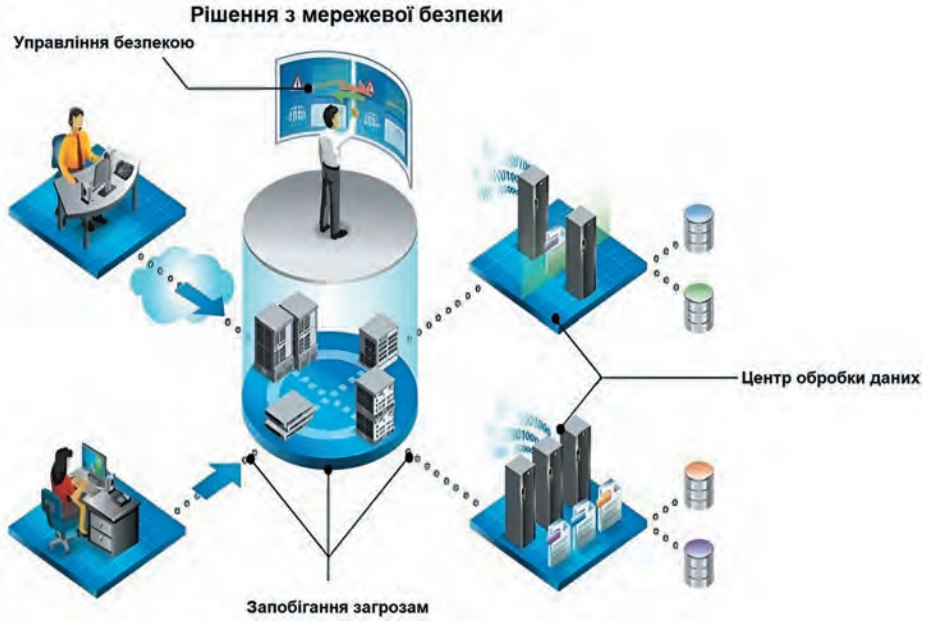

Рис. 1. Захист від кіберзагроз — комплексне рішення

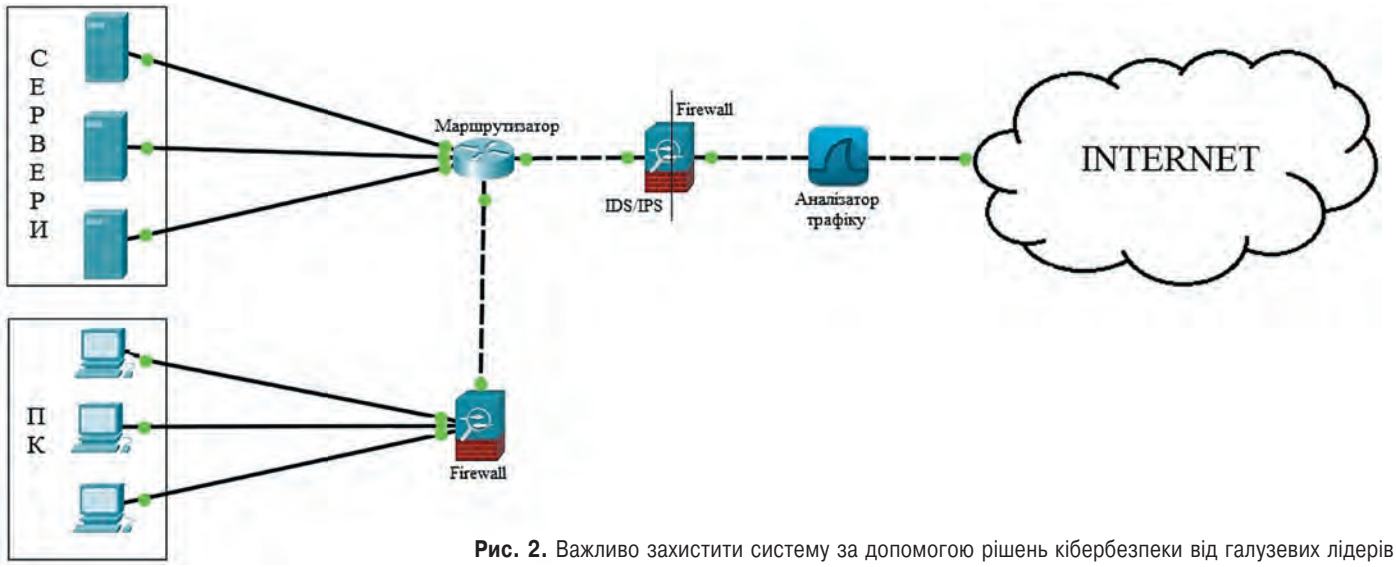

Рис. 2. Важливо захистити систему за допомогою рішень кібербезпеки від галузевих лідерів

точок, які використовують машинне навчання для виявлення та блокування нових загроз.

4. Четвертий етап вторгнення зловмисника – це встановлення так званого «бекдору» у скомпрометовану систему. Для виявлення такої діяльності потрібно постійно контролювати та моніторити мережеву активність на наявність будь-яких незвичайних моделей відправлення даних, зокрема на відомі шкідливі IP-адреси.

5. Дії зловмисника щодо намічених цілей – це фактично остання стадія завдання шкоди замовнику та його системі IP-відеоспостереження. Дії на упередження загрози – регулярний аудит системи та резервне копіювання даних – можуть обмежити шкоду та пришвидшити відновлення в разі успішного нападу зловмисника.

Захищаймо камери та програми

Захист IP-камер систем відеоспостереження дуже важливий, оскільки самі відеокамери можуть служити шлюзом для проникнення зловмисників. В нашому випадку є суттєвий недолік, пов'язаний безпосередньо з передачею незашифрованих даних, які можуть бути перехоплені та переглянуті зловмисниками. Цю вразливість необхідно усунути, щоб зменшити пов'язані з нею ризики. Крім того, небезпечними також можуть бути мобільні застосунки на телефонах, в яких встановлено програми виробників IP-відеокамер систем відеоспостереження, зокрема засоби віддаленого моніторингу; через відсутність у них надійного захисту вони можуть служити простими точками входу для зловмисників.

Щоб запобігти несанкціонованому доступу, важливо реалізовувати надійні протоколи автентифікації. Покладаючись на паролі за замовчуванням, маємо критичну вразливість мобільних застосунків, які виконують функції моніторингу систем IP-відеоспостереження; цих слабких місць слід уникати. Для забезпечення надійного захисту потрібно використовувати двофакторну автентифікацію: перший «фактор» – це звичайний захищений пароль, стандартний для будь-якого облікового запису, відповідно до корпоративної політики безпеки. Другий «фактор» – код підтвердження, отриманий від окремої програми на мобільному пристрої чи комп'ютері.

Щоб пом'якшити наслідки атаки, треба захистити програмні рішення на кількох рівнях – так би мовити, створити надлишковий контроль безпеки. Таким чином, якщо зловмиснику вдасться зламати одну частину рішення, вплив на систему IP-відеоспостереження замовника буде обмежений цим конкретним сегментом, що запобігає несанкціонованому доступу до інших областей. Дана стратегія глибокого захисту служить двом цілям. По-перше, це полегшує процес аудиту, дозволяючи провести ретельне розслідування для виявлення дій зловмисника, часу здійснення цих дій та реакцій на них. По-друге, це дозволяє проводити аналіз подій вторгнення та порушення, допомагаючи адміністраторам проаналізувати деталі атаки, зрозуміти основні причини та розробити запобіжні заходи проти подібних нападів у майбутньому.

Як убезпечити систему відеоспостереження

Ось декілька простих рекомендацій щодо забезпечення стабільної роботи камер систем IP-відеоспостереження від виробника ПЗ Milestone Systems, виробника власне IP-камер AXIS та фахівців ТОВ «СІТОН ГРУП».

1. Періодично міняйте паролі в системі. Навіть якщо ще не зламали, потрібно іноді проводити зміну даних на устаткуванні. Виробники систем безпеки рекомендують це робити мінімум раз на два тижні. Це є запорукою того, що ніхто сторонній не зможе отримати доступ до ваших даних.

2. Змінюйте порти HTTP та TCP/IP. Потрібно проводити заміну стандартних портів, оскільки зловмисник часто сканує їх. Можливо встановити будь-який з портів діапазону від 1025 до 65535.

3. Проведіть активацію HTTPS/SSL. Налаштуйте протокол SSL, це дозволить провести шифрування зв'язку між обладнанням.

4. Користуйтесь UPnP. Ця функція дозволяє прокидати нестандартні віртуальні порти, що мінімізує можливість зламу.

5. Вимкніть SNMP. Якщо не користуєтеся цією функцією, необхідно вимкнути її, що підвищить безпеку.

6. Використовуйте PoE NVR. Підключаючи камери відеоспостереження, використовуйте PoE NVR, дана технологія здатна надійно захистити від зовнішніх факторів.

7. Проведіть блокування TELNET. У роутері необхідно блокувати TELNET, оскільки саме цим протоколом користуються віруси та зловмисники.

8. Встановіть IP-фільтр. У ньому залишайте адреси в білому списку, що дозволить виключити будь-які інші.

9. Проведіть заміну стандартних паролів ONVIF. Деякі камери мають складний пароль для входу в обліковий запис, але простий для ONVIF. Використовуючи цей протокол, необхідно провести заміну пароля для кабінету пристрою за допомогою програмного забезпечення ONVIF Device Manager.

10. Прокиньте порти. Необхідно використовувати порти, які потрібні для забезпечення цільової мети та виконання конкретно поставлених завдань.

11. Автоматичний вхід у Smart PSS. Якщо у вас активна ця функція, її необхідно обов'язково вимкнути. Якщо зловмисник отримає доступ до ПК, він без проблем зможе порушити систему відеоспостереження.

Виконавши наведені прості рекомендації, ви зможете забезпечити стабільне та надійне функціонування системи IP-відеоспостереження. Якщо вам потрібна детальніша консультація, можна звернутися до фахівців ТОВ «СІТОН ГРУП».

seeton

https://www.seeton.pro/